Health IT Policy Committee

A Public Advisory Body on Health Information Technology to the National Coordinator for Health IT

August 19, 2010

David Blumenthal, MD, MPP
Chair, HIT Policy Committee
U.S. Department of Health and Human Services
200 Independence Avenue, S.W.
Washington, D.C. 20201

Dear Mr. Chairman:

An important strategic goal of the Office of the National Coordinator (ONC) is to build public trust and participation in health information technology (IT) and electronic health information exchange by incorporating effective privacy and security into every phase of health IT development, adoption, and use.

A Privacy and Security "Tiger Team," formed under the auspices of the HIT Policy Committee, has met regularly and intensely since June to consider how to achieve important aspects of this goal.

The Tiger Team has focused on a set of targeted questions raised by the ONC regarding the exchange of personally identifiable health information required for doctors and hospitals to qualify for incentive payments under Stage I of the Electronic Health Records Incentives Program.

This letter details the Tiger Team's initial set of draft recommendations for the HIT Policy Committee's review and approval.

Throughout the process, the HIT Policy Committee has supported the overall direction of the Tiger Team's evolving recommendations, which have been discussed in presentations during regular Policy Committee meetings this summer. There has always been an understanding, however, that the Tiger Team would refine its work and compile a set of formal recommendations at the end of summer for the HIT Policy Committee's final review and approval.

It bears repeating: The following recommendations apply to electronic exchange of patient identifiable health information among known entities to meet Stage I of "meaningful use — the requirements by which health care providers and

hospitals will be eligible for financial incentives for using health information technology. This includes the exchange of information for treatment and care coordination, certain quality reporting to the Centers for Medicare & Medicaid Services (CMS), and certain public health reporting.

Additional work is needed to apply even this set of initial recommendations specifically to other exchange circumstances, such as exchanging data with patients and sharing information for research. We hope we will be able to address these and other key questions in the months to come.

Most importantly, the Tiger Team recommends an ongoing approach to privacy and security that is comprehensive and firmly guided by fair information practices, a well-established rubric in law and policy. We understand the need to address ad hoc questions within compressed implementation time frames, given the statutory deadlines of the EHR Incentives Program. However, ONC must apply the full set of fair information practices as an overarching framework to reach its goal of increasing public participation and trust in health IT.

I. FAIR INFORMATION PRACTICES AS THE FOUNDATION

Core Tiger Team Recommendation:
All entities involved in health information exchange – including providers[1] and third party service providers like Health Information Organizations (HIOs) and other intermediaries – should follow the full complement of fair information practices when handling personally identifiable health information.

Fair information practices, or FIPs, form the basis of information laws and policies in the United States and globally. This overarching set of principles, when taken together, constitute good data stewardship and form a foundation of public trust in the collection, access, use, and disclosure of personal information.

We used the formulation of FIPs endorsed by the HIT Policy Committee and adopted by ONC in the *Nationwide Privacy and Security Framework for Electronic Exchange of Individually Identifiable Health Information.*[2] The principles in the *Nationwide Framework* are:

[1] Our recommendations are intended to broadly apply to both individual and institutional providers.
[2] http://healthit.hhs.gov/portal/server.pt/gateway/PTARGS_0_10731_848088_0_0_18/NationwidePS_Framework-5.pdf.

- ***Individual Access*** – Individuals should be provided with a simple and timely means to access and obtain their individually identifiable health information in a readable form and format.
- ***Correction*** – Individuals should be provided with a timely means to dispute the accuracy or integrity of their individually identifiable health information, and to have erroneous information corrected or to have a dispute documented if their requests are denied.
- ***Openness and Transparency*** – There should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information.
- ***Individual Choice*** – Individuals should be provided a reasonable opportunity and capability to make informed decisions about the collection, use, and disclosure of their individually identifiable health information. (This is commonly referred to as the individual's right to consent to identifiable health information exchange.)
- ***Collection, Use, and Disclosure Limitation*** – Individually identifiable health information should be collected, used, and/or disclosed only to the extent necessary to accomplish a specified purpose(s) and never to discriminate inappropriately.
- ***Data Quality and Integrity*** – Persons and entities should take reasonable steps to ensure that individually identifiable health information is complete, accurate, and up-to-date to the extent necessary for the person's or entity's intended purposes and has not been altered or destroyed in an unauthorized manner.
- ***Safeguards*** – Individually identifiable health information should be protected with reasonable administrative, technical, and physical safeguards to ensure its confidentiality, integrity, and availability and to prevent unauthorized or inappropriate access, use, or disclosure.
- ***Accountability*** – These principles should be implemented, and adherence assured, through appropriate monitoring and other means and methods should be in place to report and mitigate non-adherence and breaches.

The concept of remedies or redress — policies formulated in advance to address situations where information is breached, used, or disclosed improperly — is not expressly set forth in this list (although it is implicit in the principle of accountability). As our work evolves toward a full complement of privacy policies and practices, we believe it will be important to further spell out remedies as an added component of FIPs.

We also note that in a digital environment, robust privacy and security policies should be bolstered by innovative technological solutions that can enhance our

ability to protect information. This includes requiring that electronic record systems adopt adequate security protections (like encryption, audit trails, and access controls), but it also extends to decisions about infrastructure and how health information exchange will occur, as well as how consumer consents will be represented and implemented. The Tiger Team's future work will need to address the role of technology in protecting privacy and security.

II. CORE VALUES

In addition to a firm embrace of FIPs, the Tiger Team offers the following set of **Core Values** to guide ONC's work to promote health information technology:

- **The relationship between the patient and his or her health care provider is the foundation for trust in health information exchange, particularly with respect to protecting the confidentiality of personal health information.**
- **As key agents of trust for patients, providers are responsible for maintaining the privacy and security of their patients' records.**
- **We must consider patient needs and expectations. Patients should not be surprised about or harmed by collections, uses, or disclosures of their information.**
- **Ultimately, to be successful in the use of health information exchange to improve health and health care, we need to earn the trust of both consumers and physicians.**

III. SPECIFIC RECOMMENDATIONS REQUESTED

ONC has asked the Tiger Team for specific recommendations in the following areas:

- Use of intermediaries or third party service providers in identifiable health information exchange;
- Trust framework to allow exchange among providers for purpose of treating patients;
- Ability of the patient to consent to participation in identifiable health information exchange at a general level (i.e., yes or no), and how consent should be implemented;
- The ability of technology to support more granular patient consents (i.e., authorizing exchange of specific pieces of information while excluding other records); and

- Additional recommendations with respect to exchange for Stage I of Meaningful Use – treatment, quality reporting, and public health reporting.

All of our recommendations and deliberations have assumed that participating individuals and entities are in compliance with applicable federal and state privacy and security laws.

We evaluated these questions in light of FIPs and the core values discussed above.

1. Policies Regarding the Use of Intermediaries/Third Party Service Providers/ Health Information Organizations (HIOs)

In the original deliberations of the Privacy and Security Work Group of the HIT Policy Committee, we concluded that directed exchange among a patient's treating providers – the sending of personally identifiable health information from "provider A to provider B" – is generally consistent with patient expectations and raises fewer privacy concerns, assuming that the information is sent securely.

However, the Tiger Team recognized that a number of exchange models currently in use are known to involve the use of intermediaries or third party organizations that offer valuable services to providers that often facilitate the effective exchange of identifiable health information ("third party service organizations"). A common example of a third party service organization is a Health Information Organization (HIO) (as distinguished from the term "health information exchange" (HIE), which can be used to refer to information exchange as a verb or a noun.) The exposure of a patient's personally identifiable health information to third party service organization raises risk of disclosure and misuse, particularly in the absence of clear policies regarding that organization's right to store, use, manipulate, re-use or re-disclose information.

Our recommendations below regarding third party service organizations aim to address the following fair information practices:

Individual Access

Correction

✔ ***Openness and Transparency***

Individual Choice

✔ ***Collection, Use, and Disclosure Limitation***

Data Quality and Integrity

Safeguards

✔ ***Accountability***

<u>Tiger Team Recommendation 1</u>: With respect to third-party service organizations:

- ***Collection, Use and Disclosure Limitation*: Third party service organizations may not collect, use or disclose personally identifiable health information for any purpose other than to provide the services specified in the business associate or service agreement with the data provider, and necessary administrative functions, or as required by law.**
- ***Time limitation*: Third party service organizations may retain personally identifiable health information only for as long as reasonably necessary to perform the functions specified in the business associate or service agreement with the data provider, and necessary administrative functions.**

  Retention policies for personally identifiable health information must be established, clearly disclosed to customers, and overseen. Such data must be securely returned or destroyed at the end of the specified retention period, according to established NIST standards and conditions set forth in the business associate or service agreement.
- ***Openness and transparency:* Third party service organizations should be obligated to disclose in their business associate or service agreements with their customers how they use and disclose information, including without limitation their use and disclosure of <u>de-identified</u> data, their retention policies and procedures, and their data security practices.[3]**

- ***Accountability:* When such third party service organizations have access to personally identifiable health information, they must execute and be bound by business associate agreements under the Health Insurance Portability and Accountability Act regulations (HIPAA).[4] However, it's not clear that those agreements have historically been sufficiently effective in limiting a third-party's use or disclosure of identifiable information, or in providing the required transparency.**

- **While significant strides have been made to clarify how business associates may access, use and disclose information received from a covered entity, business associate agreements, by themselves, do**

[3] This is the sole recommendation in this letter that also applies to data that qualifies as de-identified under HIPAA. The "Tiger Team" intends to take up de-identified data in a more comprehensive way in subsequent months.
[4] 45 CFR 164.504(e).

not address the full complement of governance issues, including oversight, accountability, and enforcement. We recommend that the HIT Policy Committee oversee further work on these governance issues.

2. Trust Framework For Exchange Among Providers for Treatment

The issue of provider identity and authentication is at the heart of even the most basic exchange of personally identifiable health information among providers for purposes of a patient's treatment. To an acceptable level of accuracy, Provider A must be assured that the information intended for provider B is in fact being sent to provider B; that providers on both ends of the transaction have a treatment relationship with the subject of the information; and that both ends are complying with baseline privacy and security policies, including applicable law.

Our recommendations below regarding trusted credentialing aim to address the following fair information practices:

Individual Access

Correction

✔ ***Openness and Transparency***

Individual Choice

Collection, Use, and Disclosure Limitation

✔ ***Data Quality and Integrity***

Safeguards

✔ ***Accountability***

Tiger Team Recommendation 2.1:

- **Accountability: The responsibility for maintaining the privacy and security of a patient's record rests with the patient's providers, who may delegate functions such as issuing digital credentials or verifying provider identity, as long as such delegation maintains this trust.**
    - **To provide physicians, hospitals, and the public with an acceptable level of accuracy and assurance that this credentialing responsibility is being delegated to a "trustworthy" organization, the federal government (ONC) has**

a role in establishing and enforcing clear requirements about the credentialing process, which must include a requirement to validate the identity of the organization or individual requesting a credential.

- **State governments can, at their option, also provide additional rules for credentialing service providers so long as they meet minimum federal requirements.**

We believe further work is necessary to develop policies defining the appropriate level of assurance for credentialing functions, and we hope to turn to this work in the fall.

A trust framework for provider-to-provider exchange also must provide guidance on acceptable levels of accuracy for determining whether both the sending and receiving provider each have a treatment relationship with the person who is the subject of the information being exchanged. Further, the trust framework should require transparency as to whether both senders and recipients are subject to baseline privacy and security policies. We offer the following recommendations on these points:

Tiger Team Recommendation 2.2:

- **Openness and transparency: The requesting provider, at a minimum, should provide attestation of his or her treatment relationship with the individual who is subject of the health information exchange.**

- **Accountability: Providers who exchange personally identifiable health information should comply with applicable state and federal privacy and security rules. If a provider is not a HIPAA-covered entity or business associate, mechanisms to secure enforcement and accountability may include:**

  - **Meaningful user criteria that require agreement to comply with the HIPAA Privacy and Security Rules;**

  - **NHIN conditions of participation;**

  - **Federal funding conditions for other ONC and CMS programs; and**

  - **Contracts/Business Associate agreements that hold all participants to HIPAA, state laws, and any other policy requirements (such as those that might be established as the terms of participation).**

- **Openness and transparency: Requesting providers who are not covered by HIPAA should disclose this to the disclosing provider before patient information is exchanged.**

3. <u>Right of the patient or provider to consent to identifiable health information exchange at a general level — and how are such consents implemented</u>

The Tiger Team was asked to examine the role that <u>one</u> of the fair information practices - individual choice or patient consent – should play in health information exchange. The recommendations cover the role of consent in directed exchange, triggers for when patient consent should be required (beyond what may already be required by law), the form of consent, and how consent is implemented. We also set forth recommendations on whether providers should be required to participate in certain forms of exchange. We must emphasize that looking at one element of FIPs in isolation is not optimal and our deliberations have assumed strong policies and practices in the other elements of FIPs required to support the role of individual consent in protecting privacy.

Our recommendations below regarding patient consent aim to address the following fair information practices:

Individual Access

Correction

Openness and Transparency

✔ ***Individual Choice***

Collection, Use, and Disclosure Limitation

Data Quality and Integrity

Safeguards

Accountability

A. <u>Consent and Directed Exchange</u>

<u>Tiger Team Recommendation 3.1:</u>

- **Assuming FIPs are followed, directed exchange <u>for treatment</u> does not <u>require</u> patient consent beyond what is required in current law or what has been customary practice.**

Our recommendation about directed exchange is not intended to change the patient-provider relationship or the importance of the provider's judgment in evaluating which parts of the patient record are appropriate to exchange for a

given purpose. The same considerations and customary practices that apply to paper or fax exchange of patient health information should apply to direct electronic exchange. As always, providers should be prepared and willing to discuss with patients how their information is disclosed; to take into account patients' concerns for privacy; and also ensure the patient understands the information the receiving provider or clinician will likely need in order to provide safe, effective care.

B. Trigger for Additional Patient Consent

Tiger Team Recommendation 3.2:

- **When the decision to disclose or exchange the patient's identifiable health information from the provider's record is not in the control of the provider or that provider's organized health care arrangement ("OHCA"),[5] patients should be able to exercise *meaningful consent* to their participation. ONC should promote this policy through all of its levers.**
  - **Examples of this include:**
    - **A health information organization operates as a centralized model, which retains identifiable patient data and makes that information available to other parties.**
    - **A health information organization operates as a federated model and exercises control over the ability to access individual patient data.**
    - **Information is aggregated outside the auspices of the provider or OHCA and comingled with information about the patient from other sources.**

---

[5] *Organized health care arrangement* (45 CFR 160.103) means:
(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
(2) An organized system of health care in which more than one covered entity participates and in which the participating covered entities:
(i) Hold themselves out to the public as participating in a joint arrangement; and
(ii) Participate in joint activities that include at least one of the following:
(A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
(B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
(C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
[provisions applicable to health plans omitted]

- **As we have noted previously, the above recommendation on consent applies to Stage 1 Meaningful Use (thus, if consent applies, it applies to exchange for treatment). We will need to consider potential additional triggers when we start to discuss exchange beyond Stage One of Meaningful Use.**

- **An important feature of meaningful consent criteria, outlined further below, is that the patient be provided with an opportunity to give meaningful consent before the provider releases control over exchange decisions. If the patient does not consent to participate in an HIO model that "triggers" consent, the provider should, alternatively, exchange information through directed exchange. There are some HIOs that offer multiple services. The provider may still contract with an HIO to facilitate directed exchange as long as the arrangement meets the requirements of recommendation 1 of this letter.**

C. Form of Consent

Consent in our discussions refers to the process of obtaining permission from an individual to collect, use or disclose her personal information for specified purposes. It is also an opportunity to educate consumers about the decision, its potential benefits, its boundaries, and its risks.

While the debate about consent often devolves into a singularly faceted discussion of opt-in or opt-out, we have come to the conclusion that both opt-in and opt-out can be implemented in ways that fail to permit the patient to give meaningful consent. For example, consider the case in which patients are provided with opt-in consent, but the exercise of consent and education about it are limited – the registration desk provides the patient with a form that broadly describes all HIO uses and disclosures and the patient is asked to check a box and consent to all of it. As another example, consider the case in which patients have a right to opt-out – but the patient is not provided with time to make the decision and information about the right or how to exercise it can only be found in a poster in the provider's waiting room or on a page of the HIO's website. It would jeopardize the consumer trust necessary for HIOs to succeed to simply provide guidance to use "opt-in" or "opt-out" without providing additional guidance to assure that the consent is meaningful.

Tiger Team Recommendation 3.3: Meaningful Consent Guidance When Trigger Applies

In a circumstance where patient's consent is "triggered," such consent must be meaningful[6] in that it:

- **Allows the individual advanced knowledge/time to make a decision. (e.g., outside of the urgent need for care.)**
- **Is not compelled, or is not used for discriminatory purposes. (e.g., consent to participate in a centralized HIO model or a federated HIO model is not a condition of receiving necessary medical services.)**
- **Provides full transparency and education. (I.e., the individual gets a clear explanation of the choice and its consequences, in consumer-friendly language that is conspicuous at the decision-making moment.)**
- **Is commensurate with the circumstances. (I.e., the more sensitive, personally exposing, or inscrutable the activity, the more specific the consent mechanism. Activities that depart significantly from patient reasonable expectations require greater degree of education, time to make decision, opportunity to discuss with provider, etc.)**
- **Must be consistent with reasonable patient expectations for privacy, health, and safety; and**
- **Must be revocable. (i.e., patients should have the ability to change their consent preferences at any time. It should be clearly explained whether such changes can apply retroactively to data copies already exchanged, or whether they apply only "going forward.")**

D. Consent Implementation Guidance

Further considerations for implementation includes the following guidance:

Tiger Team Recommendation 3.4 :

- **Based on our core values, the person who has the direct, treating relationship with the individual, in most cases the patient's provider, holds the trust relationship and is responsible for educating and**

[6] http://www.connectingforhealth.org/phti/reports/cp3.html

discussing with patients about how information is shared and with whom.

- **Such education should include the elements required for meaningful choice, as well as understanding of the "trigger" for consent (i.e., how information is being accessed, used and disclosed).**
- **The federal government has a significant role to play and a responsibility to educate providers and the public (exercised through policy levers).**
- **ONC, regional extension centers, and health information organizations should provide resources to providers, model consent language, and educational materials to demonstrate and implement meaningful choice. HIOs should also be transparent about their functions/operations to both providers and patients.**
- **The provider/provider entity is responsible for <u>obtaining</u> and keeping track of patient consent (with respect to <u>contribution</u> of information from their records.) However, the provider may delegate the management/administrative functions to a third party (such as an HIO), with appropriate oversight.**

E. <u>Provider Consent to Participate in Exchange</u>

The Tiger Team was asked whether providers should have a choice about participating in exchange models.

<u>Tiger Team Recommendation 3.5</u>: Yes! Based on the context of Stage I Meaningful Use, which is a voluntary program, ONC is not requiring providers to participate in any particular health information exchange.

4. <u>The current ability of technology to support more granular patient consents.</u>

Our recommendations below regarding granular consent aim to address the following fair information practices:

Individual Access

Correction

Openness and Transparency

✔ ***Individual Choice***

Collection, Use, and Disclosure Limitation

Data Quality and Integrity

Safeguards

Accountability

In making recommendations about granular consent and sensitive data, we have the following observations:

- All health information is sensitive, and what patients deem to be sensitive is likely to be dependent on their own circumstances.

- However, the law recognizes some categories of data as being more sensitive than others.

- Unless otherwise required by law and consistent with our previous recommendation 3.1, with respect to directed exchange for treatment, the presence of sensitive data in the information being exchanged does not trigger an additional requirement to obtain the patient's consent in the course of treating a patient.

- Our recommendations on consent do not make any assumptions about the capacity for an individual to exercise granular control over their information. But since this capability is emerging and its certainly fulfills the aspiration of individual control, we sought to understand the issue in greater depth.

- The Tiger Team considered previous NVHS letters and received a presentation of current NCVHS efforts on sensitive data. We also held a hearing on this topic to try to understand whether and how current EHR technology supports the ability for patients to make more granular decisions on consent – in particular, to give consent to the providers to transmit only certain parts of their medical record.

- We learned that many EHR systems have the capability to suppress psychotherapy notes (narrative). We also learned that some vendors offer the individual the ability to suppress specific codes. We believe this is promising. With greater use and demand, this approach could possibly drive further innovations.

- We also note, however, that the majority of witnesses with direct experience in offering patients the opportunity for more granular control indicated that most patients[7] agreed to the use of their information generally and did not exercise granular consent options when offered the opportunity to do so. The Tiger Team also learned that the filtering methodologies are still evolving and improving, but that challenges remain,

[7] Witnesses offered estimates of greater than 90%.

particularly in creating filters that can remove any associated or related information not traditionally codified in standard or structured ways.

- While it is common for filtering to be applied to some classes of information by commercial applications based on contractual or legal requirements, we understand that most of the commercial EHR systems today do not provide this filtering capability at the individual patient level. There are some that have the capability to allow the user to set access controls by episode of care/encounter/location of encounter, but assuring the suppression of all information generated from a particular episode (such as prescription information) is challenging.

- Preventing what may be a downstream clinical inference is clearly a remaining challenge and beyond the state of the art today. Even with the best filtering it is hard to guarantee against "leaks."

- The Tiger Team believes that methodologies and technologies that provide filtering capability are important in advancing trust and should be further explored. There are several efforts currently being piloted in various stages of development. We believe communicating with patients about these capabilities today still requires a degree of caution and should not be over sold as fail-proof, particularly in light of the reality of downstream inferences and the current state of the art with respect to free text. Further, communicating to patients the potential implications of fine-grained filtering on care quality remains a challenge.

- We acknowledge that even in the absence of these technologies, in very sensitive cases there are instances where a completely separate record may be maintained and not released (abortion, substance abuse treatment, for example). It is likely that these practices will continue in ways that meet the expectations and needs of providers and patients.

- In our ongoing deliberations, we discussed the notion of consent being bound to the data such that it follows the information as it flows across entities. We know of no successful large-scale implementation of this concept in any other sector (in that it achieved the desired objective), including in the case of digital rights management (DRM) for music. Nonetheless, we understand that work is being done in this emerging area of technology, including by standards organizations.

- While popular social networking sites are exploring allowing users more granular control (such as Facebook), the ability of individuals to exercise this capability as intended is still unclear.[8] In addition, the data that

[8] See http://www.nytimes.com/2010/05/13/technology/personaltech/13basics.html and http://www.nytimes.com/interactive/2010/05/12/business/facebook-privacy.html.

populates a Facebook account is under the user's control and the user has unilateral access to it. Health data is generated and stored by myriad of entities in addition to the patient.

- Even the best models of PHRs or medical record banks provide individuals with control over copies of the individual's information. They do not provide control over the copy of the information under the provider's control or that is generated as a part of providing care to the patient. They also do not control the flow of information once the patient has released it or allowed another entity to have access to it.

- Discussions about possible or potential future solutions were plentiful in our deliberations. But the Tiger Team believes that solutions must be generated out of further innovation and, critically, testing of implementation experience.

- The Tiger Team also considered previous NCVHS letters and received a presentation of current NCVHS efforts on sensitive data.

- The Tiger Team therefore asked whether and what actions ONC might take to stimulate innovation and generate more experience about how best to enable patients to make more granular consent decisions.

Tiger Team Recommendation 4: Granular Consent

- **The technology for supporting more granular patient consent is promising but is still in the early stages of development and adoption. Furthering experience and stimulating innovation for granular consent are needed.**

- **This is an area that should be a priority for ONC to explore further, with a wide vision for possible approaches to providing patients more granular control over the exchange and use of their identifiable health information, while also considering implications for quality of care and patient safety, patient educational needs, and operational implications.**

- **The goal in any related endeavor that ONC undertakes should not be a search for possible or theoretical solutions but rather to find evidence (such as through pilots) for models that have been implemented successfully and in ways that can be demonstrated to be used by patients and fulfill their expectations. ONC and its policy advising bodies should be tracking this issue in an ongoing way and seeking lessons learned from the field as health information exchange matures.**

- **In the interim, and in situations where these technical capabilities are being developed and not uniformly applied, patient education is paramount: Patients must understand the implications of their decisions and the extent to which their requests can be honored, and we encourage setting realistic expectations. This education has implications for providers but also for HIOs and government.**

5. **<u>Exchange for Stage 1 of Meaningful Use – Treatment, Quality reporting, Public health reporting</u>**

   Our additional recommendations below regarding Stage 1 of Meaningful Use aim to address the following fair information practices:

   Individual Access

   Correction

   Openness and Transparency

   ✔ ***Individual Choice***

   ✔ ***Collection, Use, and Disclosure Limitation***

   Data Quality and Integrity

   Safeguards

   Accountability

<u>Tiger Team Recommendation 5:</u>

- **Individual Consent: The exchange of identifiable health information for "treatment" should be limited to treatment of the individual who is the subject of the information, unless the provider has the consent of the subject individual to access, use, exchange or disclose his or her information to treat others. (We note that this recommendation may need to be further refined to ensure the appropriate care of infants or children when a parent's or other family members information is needed to provide treatment and it is not possible or practical to obtain even a general oral assent to use a parent's information.)**
- **Collection, Use and Disclosure Limitation: Public health reporting by providers (or HIOs acting on their behalf) should take place using the least amount of identifiable data necessary to fulfill the lawful public health purpose for which the information is being sought. Providers should account for disclosure per existing law. More sensitive identifiable data should be subject to higher levels of protection.**

- **In cases where the law requires the reporting of identifiable data (or where identifiable data is needed to accomplish the lawful public health purpose for which the information is sought), identifiable data may be sent. Techniques that avoid identification, including pseudonymization, should be considered, as appropriate.**

- **Collection, use and Disclosure Limitation: Quality data reporting by providers (or HIOs acting on their behalf) should take place using the least amount of identifiable data necessary to fulfill the purpose for which the information is being sought. Providers should account for disclosure. More sensitive identifiable data should be subject to higher levels of protection.**
- **The provider is responsible for disclosures from records under its control, but may delegate lawful quality or public health reporting to an HIO (pursuant to a business associate agreement) to perform on the provider's behalf; such delegation may be on a "per request" basis or may be a more general delegation to respond to all lawful requests.**

IV. CONCLUSION

The foregoing recommendations were targeted to address set of questions raised by ONC. They should not be taken as the definitive or final word on privacy and security and health IT/health information exchange; they are instead a set of concrete steps that the Tiger Team believes are critical to establishing and maintaining trust. As we have said from the outset, these recommendations can only deliver the trust necessary when they are combined with the full implementation of all the FIPs. Only a systemic and comprehensive approach to privacy and security can achieve confidence among the public. In particular, our recommendations do not address directly the need to also establish individual access, correction and safeguards capabilities, and we recommend these be considered closely in the very near future, in conjunction with a further detailed assessment of how the other FIPs are being implemented.

We look forward to continuing to work on these issues.

Sincerely,

Deven McGraw

Paul Egerman

Deven McGraw
Chair

Paul Egerman
Co-Chair

Appendix A—Tiger Team Members

Deven McGraw, Chair, Center for Democracy & Technology
Paul Egerman, Co-Chair,
Dixie Baker, SAIC
Christine Bechtel, National Partnership for Women & Families
Rachel Block, NYS Department of Health
Carol Diamond, Markle Foundation
Judy Faulkner, EPIC Systems Corp.
Gayle Harrell, Consumer Representative/Florida
John Houston, University of Pittsburgh Medical Center; NCVHS
David Lansky, Pacific Business Group on Health
David McCallie, Cerner Corp.
Wes Rishel, Gartner
Latanya Sweeney, Carnegie Mellon University
Micky Tripathi, Massachusetts eHealth Collaborative